



Ensuring integrity with fingerprint verification

Magnus Pettersson, Mårten Öbrink

Precise Biometrics AB, Dag Hammarskjölds väg 2, SE 224 67 Lund, Sweden

16th November 2001

Abstract

With the increase of online communication and transactions, the demand for security and privacy increases. There are several solutions already in use to protect confidential information and to authenticate people electronically. When biometrics is used, it often triggers a discussion concerning privacy and integrity. One major reason for this is that fingerprints from criminals are stored in police registers. The scope of this document is to explain how fingerprint verification, personal tokens and Match-On-Card technology can help ensure integrity.

1 Introduction

When a fingerprint image is enrolled, only parts of the information is stored. This information extract is called a template. It is not possible to reconstruct a fingerprint image from a template; the transformation process is non-reversible.

There are two ways to store fingerprint templates; database storage or storage in a personal token. The two ways are very different and do not work with each other. A database with fingerprint templates of criminals cannot be searched with a fingerprint template from a personal token, as the template is never allowed to leave the storage in the security context, such as a Smart Card.

This white paper explains the usage of fingerprints from an integrity point of view, and how the Match-On-Card[1] technology prevents templates stored in personal tokens to be verified towards a database of templates from criminals.

2 Biometrics prove your digital identity

Public Key Infrastructure, *PKI*, comprises all necessary functions to achieve non-repudiation, encryption, digital signing and strong authentication. Still, while PKI delivers the framework for all this functionality, the problem of verifying the users identity remains.

The main methods of verification are:

- Something you *have* - might be a key, Smart Card or other token that you use to verify your identity.
- Something you *know* - might be a PIN or password that only you know.

The problem with these two methods is that they can be borrowed or stolen. Biometrics represents the third alternative:

- Something you *are* - fingerprint, iris, voice etc.

These three methods are often combined, where as one part identifies the user, while the other verifies that the person is who he/she claims to be. E.g. a Smart Card (something you have) in combination with fingerprint verification (something you are).

Using digital certificates protected with biometrics is the best way of proving a person's identity in an open network. The biometric method most commonly used is fingerprint verification. Fingerprint verification is seen as the best solution with regards to convenience, cost efficiency and reliability[2].

3 Using fingerprints and personal tokens to protect integrity

3.1 Database storage - Identification

Databases with fingerprint templates (and often mug shots) are used by FBI, Interpol etc. as well as many immigration authorities. The idea is to check fingerprint images from people against this database when for example investigating a crime. This process is called *identification*; "We found this fingerprint on the crime scene. Let's check the data base to see if we find a match among our registered criminals...". The idea of having fingerprints collected and templates stored in a database together with information about the user is not appealing to many people. Some claim these databases are a threat to privacy.

3.2 Personal token - Verification

When talking about tokens, we often refer to Smart Cards. Smart Cards are widely used for everything from bus tickets to carrier of digital certificates, which are used to access various electronic services. The reason for using a Smart Card is that it is tamper resistant; it is very hard to hack a Smart Card. This also makes the Smart Card a suitable carrier of biometric templates. In this case the Smart Card is used for identification, and the user *verifies* the ownership of it.

For digital signing of for example a contract, the user presents the Smart card to the card reader and then puts his or her finger on the fingerprint sensor. If the presented fingerprint image matches with the template stored in the Smart Card, the contract is signed with the users cryptographic key stored in the card (See

figure 1). With the Match-On-Card technology the fingerprint is verified inside the secure environment of the Smart Card. In this case the fingerprint template stored on the Smart Card cannot be extracted. It can only be used internally by the Smart Card itself. Signing contracts or documents is only one application where the biometric verification in Smart Cards can be used. Other applications might be for example ID cards, where the user proves the validity and ownership of the ID card by biometric verification.

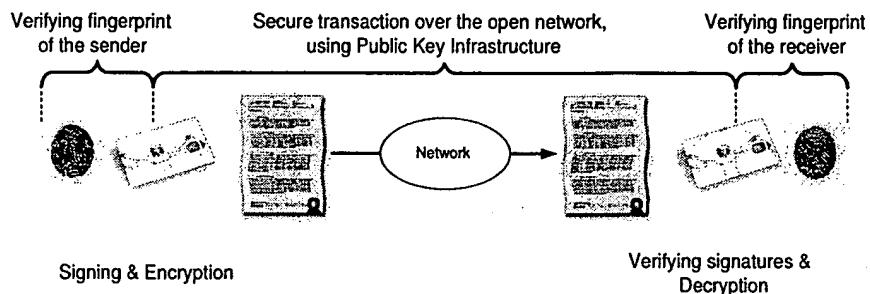


Figure 1: The figure shows an example of the usage of fingerprints for verification. The fingerprint is used to verify the ownership of the smart card, to be able to use the cryptographic keys for digital signatures and encryption.

3.3 Using Smart Cards and fingerprint verification

Referring to the conclusion presented in a report from Morgan Keegan & Co, January 2001[3], fingerprint verification is considered the most viable technology when biometrics is to be used with maintained integrity (See table 1). The only commercially proven¹ biometric technologies suitable for Smart Cards, using Match-On-Card technology, are fingerprint and voice verification, where fingerprints have far better performance with regards to accuracy. The usage of Smart Cards and Match-On-Card technology is vital for protecting biometric templates against tampering

4 Conclusion

When using biometrics in combination with a personal token, e.g. a Smart Card - no database of fingerprint templates is needed. No one has access to the stored fingerprint template, not even the owner, since the template cannot be extracted from the card. It can only be used internally in the card where it is used for matching against the fingerprint of the person who claims to be the owner of the

¹By the time of writing; November 2001.

Table 1: Ranking different biometrics (Source: Morgan Keegan & Co report January 2001[3].)

Rank	Accuarcy	Convenience	Cost	Match-On-Card
1	DNA	Voice	Voice	Finger
2	Iris	Face	Signature	Voice
3	Retina	Signature	Finger	
4	Finger	Finger	Face	
5	Face	Iris	Iris	
6	Signature	Retina	Retina	
7	Voice	DNA	DNA	

card. It is in this case not possible to misuse the fingerprint template, nor the users identity.

References

- [1] Pettersson, M., *Match-On-Card Whitepaper* 2000, Precise Biometrics external publication.
- [2] The Biometric Industry Report, ISBN 1 85617 376 3
- [3] Morgan Keegan & Co, www.morgankeegan.com
- [4] www.rsa.com
- [5] www.infineon.com
- [6] www.siemens.com
- [7] www.precisebiometrics.com

For Additional Information

www.precisebiometrics.com

Sweden, Lund

Precise Biometrics AB
Dag Hammarskjölds v.2
SE 224 64 Lund
Sweden

Tel: +46 46 311 100
Fax: +46 46 311 101
E-mail: info@precisebiometrics.com

Sweden, Stockholm

Precise Biometrics AB
Box 1223
SE 164 28 Kista
Sweden

Tel: +46 8 514 426 55
Fax: +46 8 514 426 56
E-mail: info@precisebiometrics.com

USA, Washington

Precise Biometrics Inc.
8300 Boone Boulevard, Suite 500
Vienna, VA 22182
USA

Tel: +1 703 848-9266
Fax: +1 703 832-0577
E-mail: infous@precisebiometrics.com

Entire contents ©2001 by Precise Biometrics AB. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden.